

A New Security Model for Collaborative Environments

Presenter – Deb Agarwal*

Markus Lorch**, Mary Thompson*, and Marcia
Perry*

*Lawrence Berkeley Laboratory

**Virginia Tech

Motivation



- Often a collaboration begins with just two or three members who decide to work together
- Entry into the collaboration is often through an introduction or invitation by an existing member
- Collaborators prefer to use secure systems for their interactions
- The administrator is not generally available when new people need to be added or their privileges upgraded
- Collaborators build trust in each other through interaction
- Denial of service for legitimate users has serious consequences and will lead to use of insecure systems if available or lack of adoption

Security Mechanisms



- Authentication mechanisms
 - Username/password
 - Kerberos
 - X.509 certificates
 - Public/private key pair
- Authorization mechanisms
 - Group membership (unix)
 - Access Control Lists (ACLs)
 - Authorization servers (Akenti and CAS)
- Secure communication
 - SSL/TLS
 - Grid Security Infrastructure
 - Kerberos
 - Web Services mechanisms
- All designed to require no real-time human intervention for users to gain access

Interoperation



- Cross-organization trust (same mechanisms)
 - Authentication and authorization policies
 - Security of database
- Translation gateways (map credentials between mechanisms)
 - Gridmap X.509 -> username/password
 - Gateway between Kerberos and X.509

Scenarios



- Meet a new person at a conference and want to add them to the collaboration immediately
- On travel and need to attend a meeting but your only Internet access is in an Internet café
- At a conference and start a discussion that you would like to use collaborative tools to continue
- Long-term evolving collaboratory that is crossorganizational

Requirements



- Ability to access from anywhere including Internet cafés
- Low threshold for entry into the system
 - Incorporate new users easily
 - Small amount of software downloads
 - No waiting for authorization to enter the system
- Components able to require only the level of authentication and authorization they need. E.g.
 - Weak or no authentication to enter the lobby
 - Strong authentication and authorization for sensitive actions
- Minimize dependence on servers (particularly while the collaboration is small in number)

Scenarios Revisited



- Trusted user accessing from a machine with X.509 credentials
- Trusted user connecting with username and password
- Trusted user connecting without X.509 or password access
- New user wishing to join a single session
- New user that wants to join and start collaborating
- Group of users that want to spontaneously create a collaboration

Registration Model



- Registration methods
 - Self
 - Trusted user
 - Administrator
- Registry user information
 - User name
 - Password
 - X.509 credential
 - Organizational affiliations
 - Group affiliations
 - Method of registration

Authentication Model



- A user has multiple means of authentication
- Authentication for a particular session based on
 - Location
 - Methods available
 - Security of local machine
 - Availability of connection to servers
- Authentication method for a session a property of a user's session
- Authentication method considered in authorization

Crossing the borders

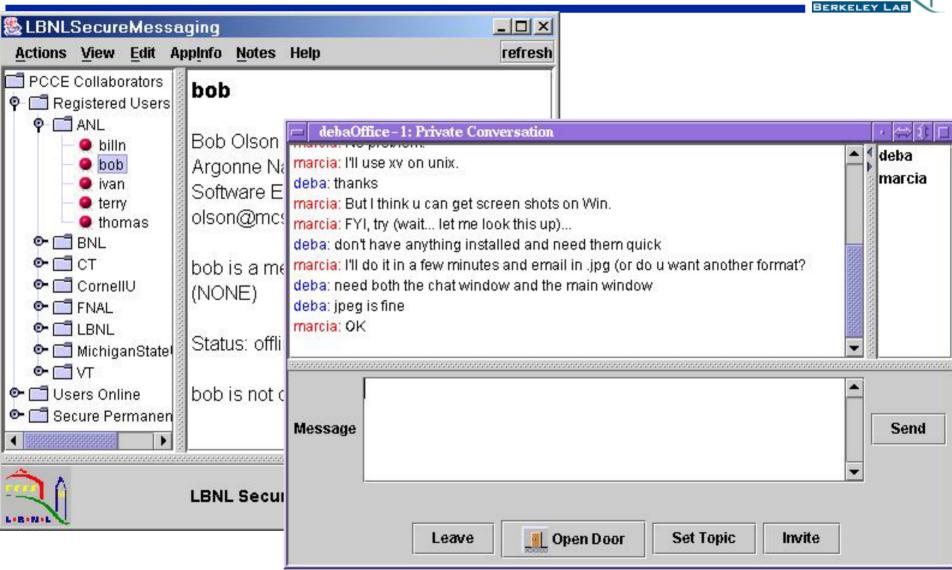


Escort

- Chaperone a user in an area they are not normally authorized to access
- Only provides privileges of the host or less
- Host able to control the guest's access
- Vouching
 - A user vouches for a less privileged user
 - Temporarily elevates privileges of the vouchee
 - Vouchee able to act without escort
- Elevation of credentials
 - Registration of user's credentials to allow higher privileges – can be done by anyone with the higher credential level

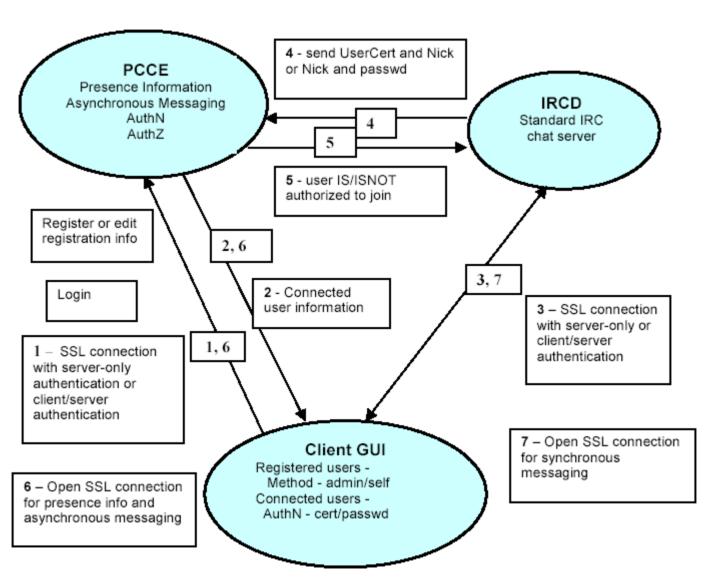
Secure Messaging





PCCE Connection Model





Authorization Issues



- Authorization decision points/coordination
 - Joining a private conversation
 - Entering a shared venue
 - Looking at files/shared date
- Authorization decision needs to take into account
 - Method of registration
 - Method of authentication
 - Vouching information
- Escort affect on authorization
 - Filter escorted user's access to real-time information
- Limitation of access granted by vouching

Issues



- Hierarchical ordering of authentication methods
- Communication method to connect users that are authenticated at different levels
- Cross-organization authentication
 - Easier
 - Harder
- Authorization complexity
 - Policy language to support this model
- Registration of credentials
 - By user
 - Administrator/trusted user vetting